online, shared file system for multiple users to access over a computer network. Other implementations of a shared storage service also can be used.

Referring to FIG. **1**, a shared storage system **100** includes one or more server computers **102** on which the storage system is hosted by a service provider. Files **120** are stored on one or more storage devices **106** that are accessed by the server computers **102**. Users access files stored on the shared storage system through client computers **104** that connect to the server computer **102** over a computer network **108**. In one implementation, the shared storage system in an online, networked storage system, such as a storage service provided to end users over the Internet. Each of the server computers and client computers can be implemented using a computing device such as described below in connection with FIG. **6**.

The client computer **104** typically includes a browser application that communicates with the server computers **102** using a conventional communication protocol. Typically, the server computer **102** prompts the user for authentication information to access an account. After receiving the authentication information and successfully authenticating the user, the server computer presents a user with information relating to their account, such as files and folder containing files that the user has stored on the shared storage system. Other operations also can be made available, such as uploading, deleting, modifying and downloading files and folders, defining collections of files, sharing files and collections of files with other users, accessing files and collections of files shared by other users, and searching for files and folders, according to a user's access privileges. In general, a client computer **104** sends requests **110** for information to the server computers **102**, in response to which the server computers provide file data **112** to the client computer **104**, where the file data **112** can be metadata about a file or contents of a file. The server computers maintain, store, update and access account information **140** about a user **142**, including information indicative of access privileges **144**, such as whether the account is enabled, whether sharing of files is enabled and the like.

A file **120** has information stored about it that the server computers **102** use to manage access to the file by various users. Each file **120** has, in particular, an access control list **122** and a prohibited content flag **124**. The access control list **122** indicates which users are permitted to access a file, and the nature of those permissions.

As described in more detail below, the prohibited content flag **124** indicates whether the file is determined to have prohibited content. Such a determination typically is made, for example, in response to a request by a third part that the content be removed. For example, a party may inform the service provider that a particular file has been identified as including copyrighted content, and the user having the file stored in his or her account is unauthorized to distribute it.

When one or more files are determined to include prohibited content, then an incident is recorded as part of an offense history **146** for the user account. This offense history **146** is accessed by an offense history processing module **148**, which can modify the access privileges **144** of the user.

A file can include one or more independently accessible portions, or file streams, which contain different information. In particular a file can include content and metadata about that content in separately accessible portions of the file. The access control list can differentiate access for users at the file stream level in addition to the file level. The access control list also can distinguish between an "owner" of a file system object and others. In one implementation, the system can limit access to prohibited content by others, while allowing full access to the owner of a file system, regardless of whether the file system object is marked as having prohibited content.

Given this context, an example implementation will be described in more detail in connection with FIGS. **2-5**.

FIG. **2** illustrates a data flow diagram of a system in which content can be shared by one user with another user through a shared storage system such as shown in FIG. **1**. Content **200** is handled by an uploading module **202** and then stored in storage **204**. Through the uploading module, a user can identify content to be uploaded, and navigate to a storage folder on the shared storage system in which to store the uploaded content. The uploading module causes the uploaded content to be stored. Access control lists **206** are created that associate the content with this user and otherwise specify permissions for various entities that can access this content.

For a user to share information, a sharing module **210** is accessed. In response to user input **212**, one or more items of stored content are identified by the user. Also though the sharing module, through user input **212**, a user can identify one or more other users with whom the selected content is to be shared. The sharing module **210** creates a collection of the selected content, and indicates on the access control list for the collection that the other identified users are authorized to access this content. A user can be an individual, a device, a system process, an application or other entity that can access content through the storage system. There are a variety of ways in which a user can specify such a collection, the users with whom it is to be shared, and the permissions to be given to those users, the foregoing merely being one example.

A content blocking module **220** can receive indications **222** of content to be blocked due to prohibited content. For example, such information can be reported by other parties. The access control list for that content is updated to indicate that there is prohibited content to be blocked when shared. The content blocking module, or other program module (not shown), also updates the offense history **246** of a user when content is marked as prohibited. An offense history processing module **240** uses rules **242** to determine whether user privileges **244** for a user should be modified based on the incidents in the offense history **246**.

Through an access module **230**, other users can access content in collections to which they have been given authorization. Given an indication **232** of an object, such as a file, to be accessed, the access module determines whether the user is authorized to access the selected content, and determines if the content is blocked, by using the access control list. If the user is authorized to access the content, the content is provided to the user. In the event that the user is authorized, but the content is blocked, a graphical user interface of the access module can indicate to the user that the content is present but access to the content is blocked.

FIG. **3** is a flowchart describing an example implementation of operation of such a system when uploading content.

A system receives **300** a request from a user to access his or her account. After allowing access, the system can receive **302** a request from the user to upload content to the storage. If the user's access has already been limited due to being a repeat offender, such access might not be provided. The system receives, processes and stores **304** the content in the storage system, including creating **306** the access control list for each file which is uploaded. The access control list can initially indicate that the user is the owner of the content and